Integrar pfSense con IPA server

Arcadio Ortega Reinoso

Este documento está bajo licencia:

Atribución – No Comercial – Compartir Igual (CC BY-NC-SA 4.0)
Puedes compartir, copiar, redistribuir y adaptar esta obra con fines no comerciales,
siempre que cites al autor y mantengas esta misma licencia para cualquier derivado.

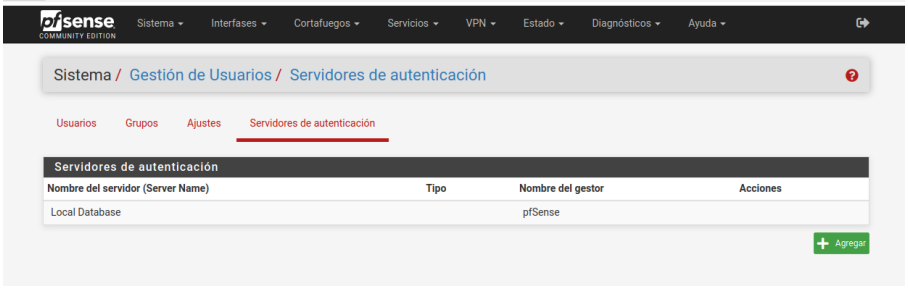
pfsense. IPA server.

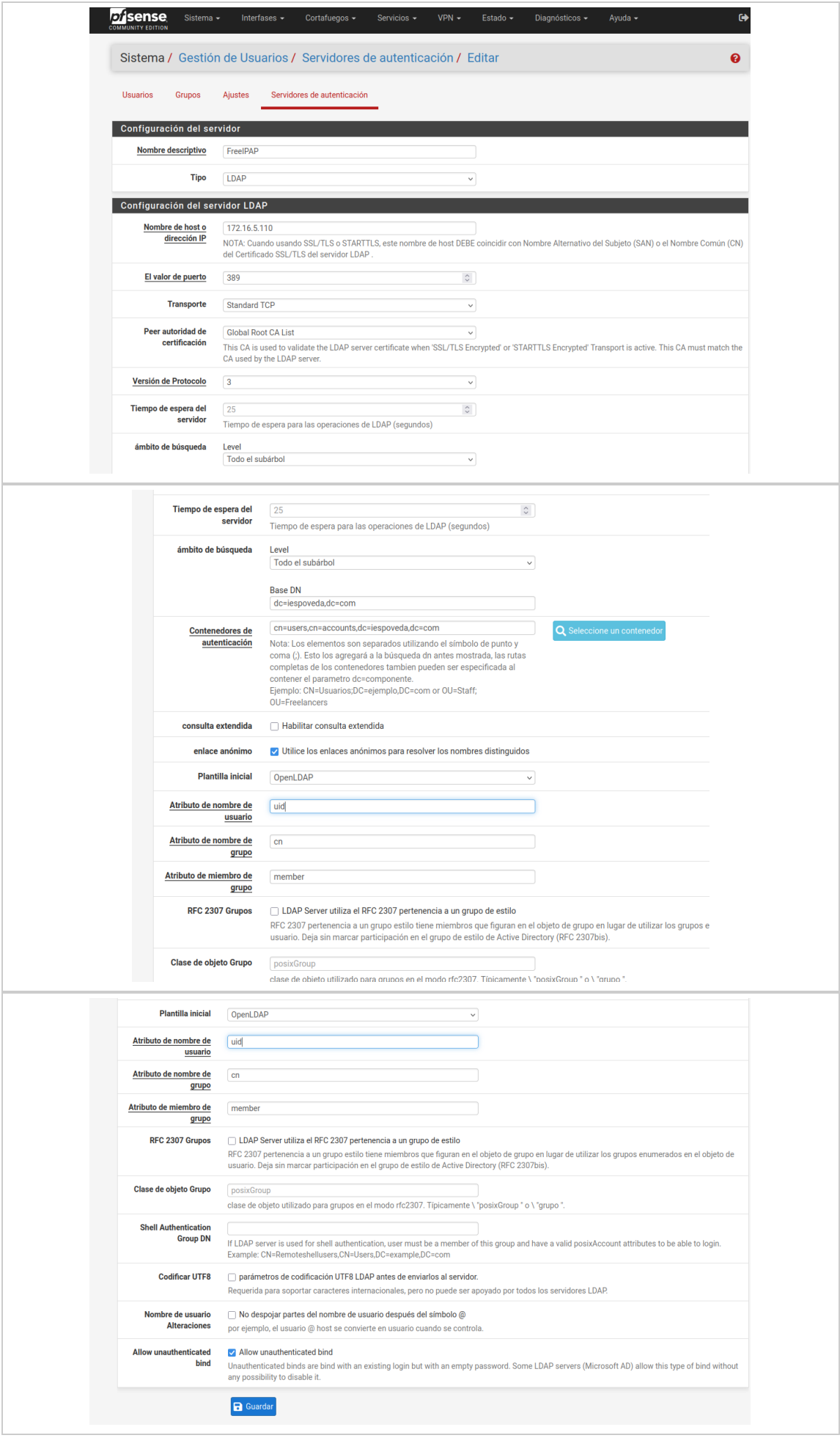
- Autenticación centralizada. Permite que los usuarios del dominio IPA inicien sesión en la interfaz web de pfSense o usen VPN (OpenVPN/IPsec) con sus credenciales de red.
- Gestión de acceso basada en grupos. Ejemplo Restringir el acceso a pfSense por grupo
- Simplificación administrativa. No necesitas crear usuarios locales en pfSense; todo se maneja desde FreeIPA.

Integración

Activar y configurar el servidor LDAP en pfSense

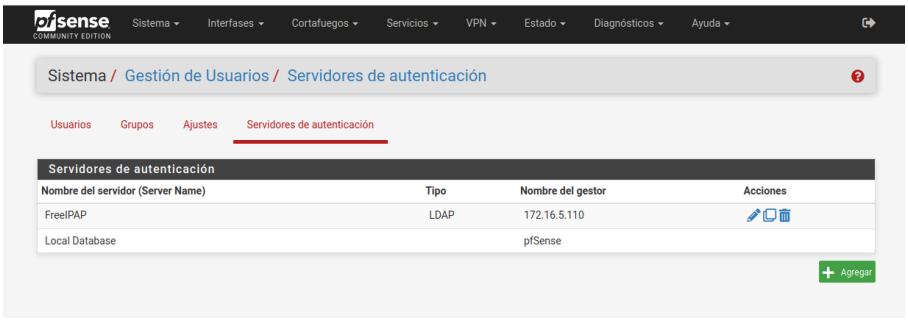
- System → User Manager → pestaña Authentication Servers.
- + Add.
- En Type, elige LDAP.
- Hostname or IP: dirección de tu servidor IPA
- Port: 389 (LDAP) o 636 (LDAPS)
- Transport: TCP - Standard o SSL (si usas LDAPS)
- Peer Certificate: si usas TLS, puede que necesites importar el CA de IPA
- Search Scope: Entire Subtree
- Base DN: Ej. dc=example,dc=com
- Authentication Containers: como cn=users,cn=accounts,dc=example,dc=com
- Bind Credentials: un usuario de FreeIPA con permisos para hacer búsquedas LDAP
- User naming attribute: generalmente uid
- Group naming attribute: generalmente cn
- Group member attribute: member
- Guarda y prueba la conexión usando el botón Select a user.

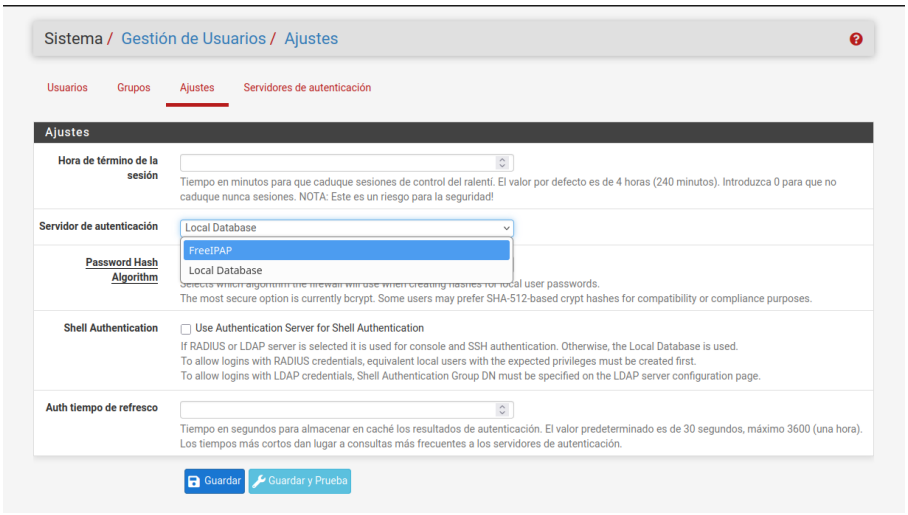


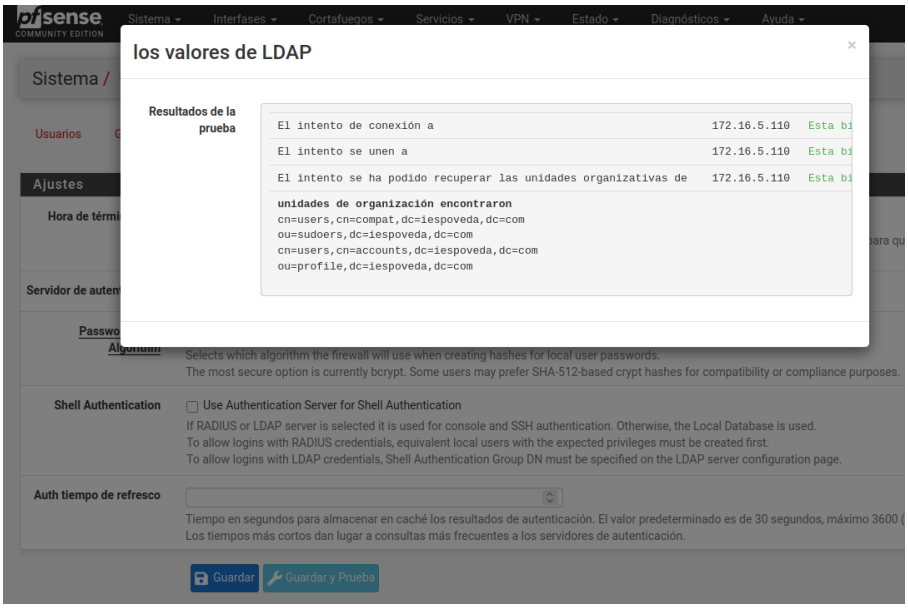


Usar FreeIPA para autenticación web o VPN

- Ve a System → User Manager → pestaña Settings.
- En "Authentication Server", selecciona tu servidor LDAP (FreeIPA).
- Aplica cambios.







Luego, puedes usar los usuarios de FreeIPA para iniciar sesión en:

- Interfaz web de pfSense
- OpenVPN (si configuras la VPN para usar ese backend)

Limitaciones y consejos

- Cambio de contraseñas No se puede cambiar la contraseña de FreeIPA desde pfSense

- Certificados Si usas LDAPS, asegúrate de importar correctamente el CA de FreeIPA
- Grupos Puedes mapear grupos de FreeIPA y darles acceso granular
- Troubleshooting Usa Diagnostics > Authentication para probar el login de un usuario

Ejemplo de uso

Controlar y auditar el acceso a Internet por usuario

- **1. Autenticación en el portal cautivo** (Captive Portal, por ejemplo, Wi-Fi pública o de invitados), puedes exigir que los usuarios ingresen credenciales LDAP antes de tener acceso a Internet.
  - Evitas que usuarios no autorizados accedan.
  - Puedes registrar qué usuario navegó y cuándo (logs).
  - Compatible con múltiples zonas (por grupo LDAP).
- **2. Proxy con autenticación (Squid Proxy)** Si usas Squid (proxy) en modo explícito, puedes forzar a que los usuarios se autentiquen antes de navegar.
  - Control y visibilidad por usuario.
  - Puedes usar SquidGuard para aplicar políticas de navegación por grupo o usuario.
- **3. Acceso a la interfaz web de pfSense (GUI)**. Puedes permitir que ciertos usuarios LDAP administren pfSense.
  - Gestión centralizada de accesos administrativos.
  - No necesitas crear usuarios locales en pfSense.
- **4. VPN (OpenVPN o IPsec con EAP-RADIUS/LDAP)**. Autenticar usuarios de VPN (por ejemplo, OpenVPN) usando LDAP.
  pfSense consulta al servidor IPA para validar credenciales.
  - Gestionas accesos VPN desde FreeIPA.
  - Puedes combinar con certificados o MFA.